Proxy Gemma

1) Introduction

Le LIMS Gemma repose sur une base de données 4D serveur 7.0.5 fonctionnant sur un serveur Windows 2000 server.

Cette version de 4D est depuis longtemps dépassée, donc plus maintenue, et les développements réalisés difficilement portables vers une version plus actuelle. Le système Windows 2000 server n'est plus maintenu depuis longtemps également.

Deux licences seulement sont disponibles pour déployer ce LIMS, et il n'est pas possible d'en acheter de nouvelles.

Lors du démarrage du service 4D, un broadcast est effectué pour vérifier que la licence du produit n'est pas déjà utilisée. Si tel est le cas, le serveur se met dans un mode de démonstration en mode lecture seule.

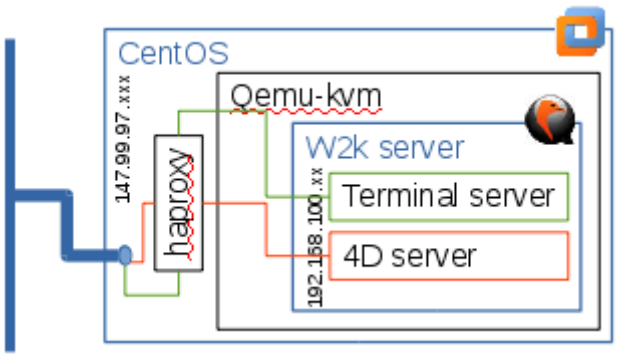
Mis à part la faiblesse sécuritaire de ce LIMS basé sur un OS et un logiciel hors maintenance et patchs de sécurité, la mise en place d'une nouvelle instance pour une espèce est de fait impossible dans l'état.

2) Solution proposée

Le but est de mettre le serveur Gemma dans un sous réseau qui lui est propre, et de le masquer ainsi des autres serveurs. Pour donner accès au service 4D ainsi qu'à une console (via RDP), il convient de mettre en place une passerelle sur un serveur à cheval sur ces deux réseaux.

Les serveurs Gemma étant virtualisés, la mise en place d'un vrai sous réseau sous-entend la création de VLAN sur les équipements réseau ainsi que la configuration de tous les serveurs du cluster de virtualisation.

Une solution plus compacte est d'utiliser le serveur faisant office de passerelle comme un serveur de virtualisation dans lequel le serveur Gemma fonctionnera sur un réseau privé. Le cluster de virtualisation vmWare autorise les « Nested VMs », il est donc possible de virtualiser le serveur passerelle lui aussi.



La solution retenue repose donc sur un serveur CentOS, avec côté virtualisation qemu-kvm, et côté

passerelle haproxy. Ce serveur aura les ports ssh(22), RDP(3389) et 4D(19813) d'ouvert.

3) Configuration CentOS

3.1) Machine virtuelle

La machine est dimensionnée pour pouvoir contenir le serveur Windows qui requiert 1 CPU, 1Go de RAM, une volumétrie disque totale de l'ordre de 54Go (34+20). Une configuration 2 CPU, 2 Go RAM et 75Go de disque a donc été retenue pour le serveur CentoS.

L'accès à la console de cette machine s'effectue via le portail Web vSphere Web Client (voir documentation Ariane https://ariane.inra.fr/block/kb_view.do?sysparm_article=KB0010266).

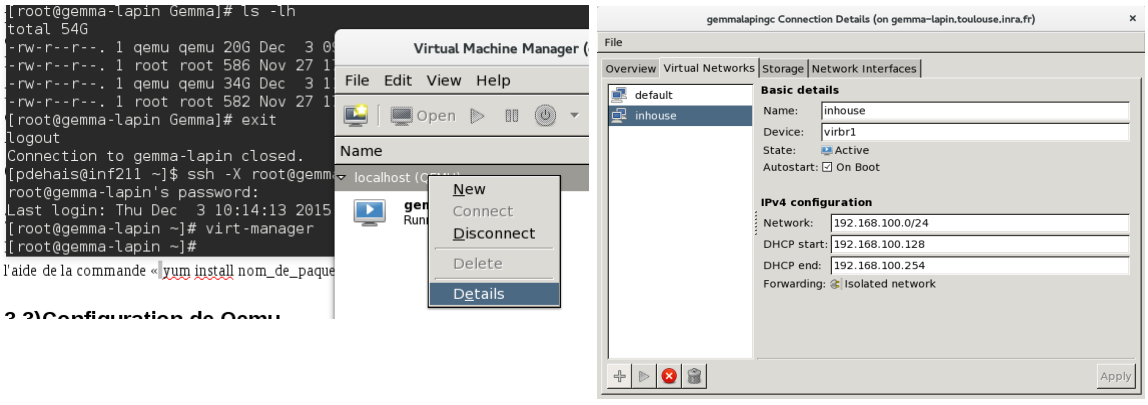
Une fois l'OS installé (serveur mini avec interface graphique, uniquement un compte root), l'administration peut se faire à l'aide d'une connexion ssh avec déport X11 (ssh -X root@nom-de-machine). Pour le mot de passe root … me le demander.

3.2) Packages

Les packages nécessaires sont gcc, kernel-devel, openssh, epel-release, virt-manager, et haproxy. Ils peuvent être installés à l'aide de la commande « yum install nom_de_paquet ».

3.3) Configuration de Qemu

Il convient de créer un sous réseau local à la machine. Pour configurer Qemu, il est possible de lancer virt-manager via une connexion ssh avec déport X11 (serveur X11 requis sur sont poste client). Un clic droit sur le nom du serveur local Qemu permet de demander le détail de sa configuration :



Un clic sur le bouton « + » permet d'ajouter un réseau.

3.4) Datastore Gemma

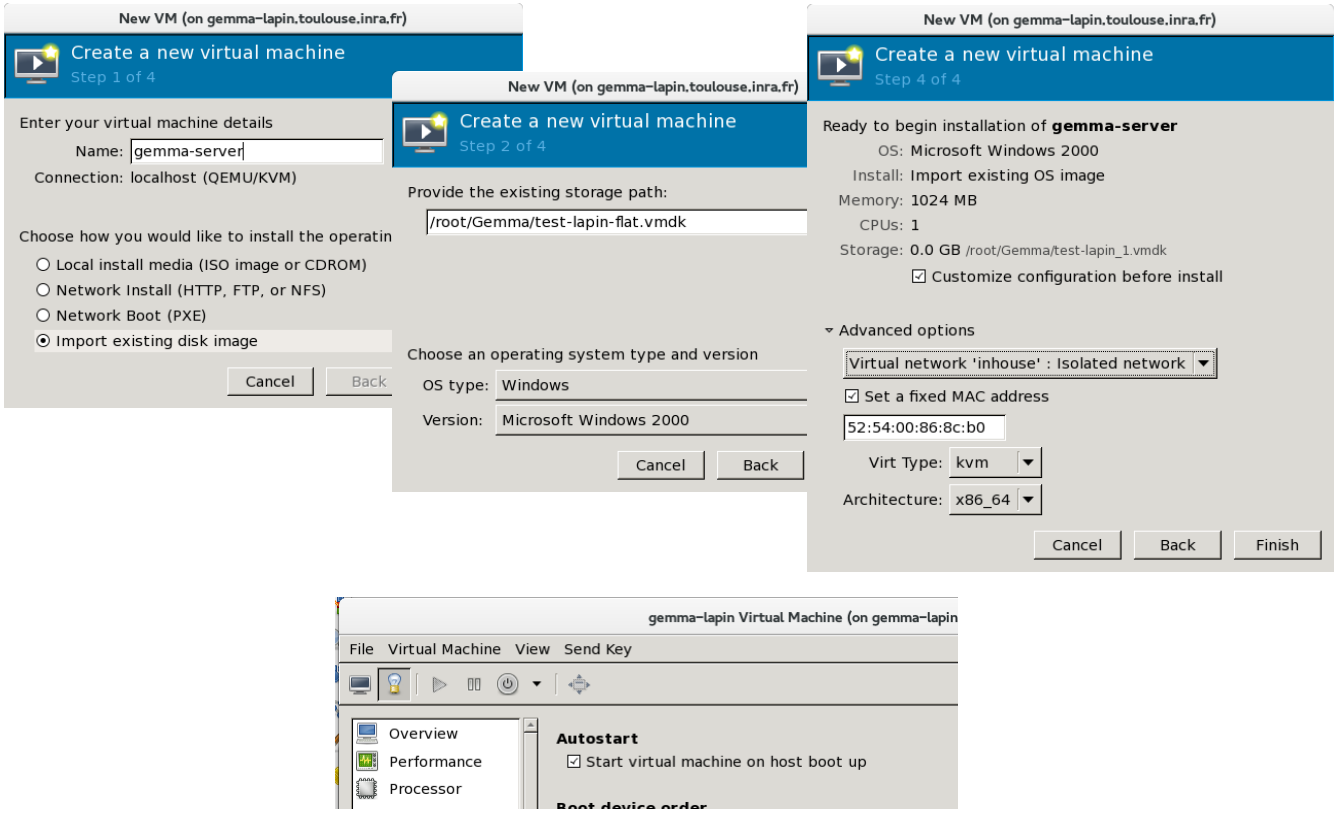
Pour stocker les futurs disques de la machine virtuelle Windows, un répertoire /root/Gemma est créé. Ces disques sont les copies des fichiers vmdk de la machine Windows virtuelle vmWare d'origine (format flat ET SANS SNAPSHOT) et copiés sur le serveur CentOS via scp.

Il est possible d'ajouter le répertoire Gemma en tant que Datastore via virt-manager de la même

manière que nous avions ajouté un réseau (onglet « Storage » cette fois-ci).

3.5) Création de la machine virtuelle Windows

La création de la machine virtuelle se fait via virt-manager, et à l'aide des disques précédemment importés et de l'interface réseau locale. Il conviendra de modifier la configuration de la machine avant de la mettre sous tension pour lui ajouter le second disque dur, et d'activer sa mise sous tension automatique.



Après modifications, la machine peut être démarrée et la configuration du système Windows modifiée via la console dans virt-manager. Il conviendra de configurer une adresse IP fixe dans la zone réseau locale (pas de gateway/passerelle), et de supprimer les vmware-tools et autres programmes qui n'ont plus lieu d'être.

3.6) Configuration de haproxy

La configuration de haproxy tient dans un seul fichier : /etc/haproxy/haproxy.cfg

```
#---------------------------------------------------------------------
# Example configuration for a possible web application.  See the
# full configuration options online.
#
#   http://haproxy.1wt.eu/download/1.4/doc/configuration.txt
#
#---------------------------------------------------------------------

#---------------------------------------------------------------------
# Global settings
#---------------------------------------------------------------------
global
    # to have these messages end up in /var/log/haproxy.log you will
    # need to:
    #
```

```
    # 1) configure syslog to accept network log events.  This is done
    #    by adding the '-r' option to the SYSLOGD_OPTIONS in
    #    /etc/sysconfig/syslog
    #
    # 2) configure local2 events to go to the /var/log/haproxy.log
    #   file. A line like the following can be added to
    #   /etc/sysconfig/syslog
    #
    #    local2.*                       /var/log/haproxy.log
    #
    log         127.0.0.1 local2

    chroot      /var/lib/haproxy
    pidfile     /var/run/haproxy.pid
    maxconn     4000
    user        haproxy
    group       haproxy
    daemon

    # turn on stats unix socket
    stats socket /var/lib/haproxy/stats

#---------------------------------------------------------------------
# common defaults that all the 'listen' and 'backend' sections will
# use if not designated in their block
#---------------------------------------------------------------------
defaults
    mode                    tcp
    timeout connect 5s
    timeout client 30ms
    timeout server 30ms
    timeout tunnel 1h

listen RPC
    bind 147.99.97.85:3389
    mode tcp
    server gemma 192.168.100.2:3389

listen 4D
    bind 147.99.97.85:19813
    mode tcp
    server gemma 192.168.100.2:19813
```

Ensuite il convient de configurer le service pour un démarrage automatique :

```
/etc/init.d/haproxy start
chkconfig –add  haproxy
chkconfig  haproxy on
```

La machine est presque prête, il faut encore désactiver le firewall via « system-config-firewall-tui ».

L'accès que se soit en ssh, RDP, ou 4D se fait avec l'adresse/DNS du serveur CentOS.

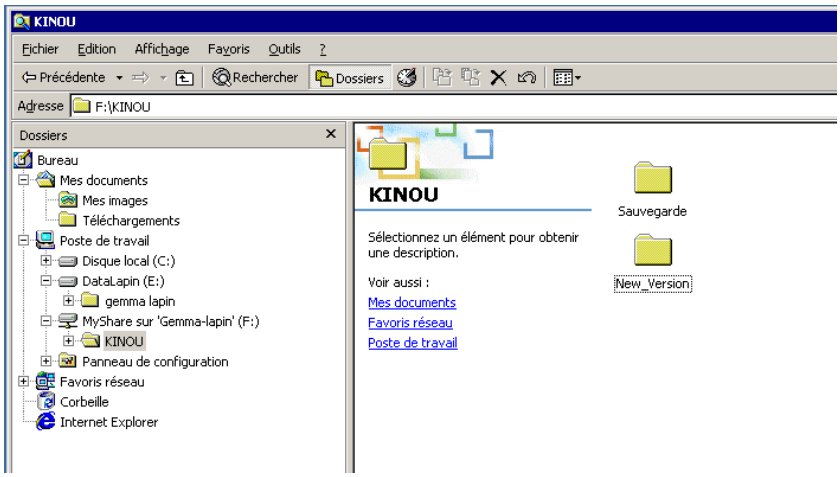
3.7) Samba share for Gemma update

Pour permettre la mise à jour de la machine Windows (copie/remplacement de fichiers), un serveur samba est mis en place pour partager le /MyShare de la machine CentOS.

```
# install
yum install samba samba-client samba-common
yum install policycoreutils-python
# config user
setsebool -P samba_domain_controller on
useradd gemmalapin
passwd gemmalapin
smbpasswd -a gemmalapin
usermod -s /sbin/nologin gemmalapin
# config folder
mkdir /MyShare
chown gemmalapin :gemmalapin /MyShare
semanage fcontext -a -t samba_share_t '/MyShare(/.*)?'
```

```
restorecon -R /MyShare

cat /etc/samba/smb.conf
#====================== Global Settings ===================================

[global]
        workgroup = MYGROUP
        hosts allow = 192.168.100.2
        security = user
        map to guest = bad user

#============================ Share Definitions ==============================

[MyShare]
        path = /MyShare/
        browsable = no
        writable = yes
        valid users = gemmalapin


chkconfig smb on
chkconfig nmb on
/etc/init.d/nmb start
/etc/init.d/smb start
```

L'accès à ce disque F : se fait donc de façon standard depuis la machine virtuelle Gemma via l'explorateur de fichiers :

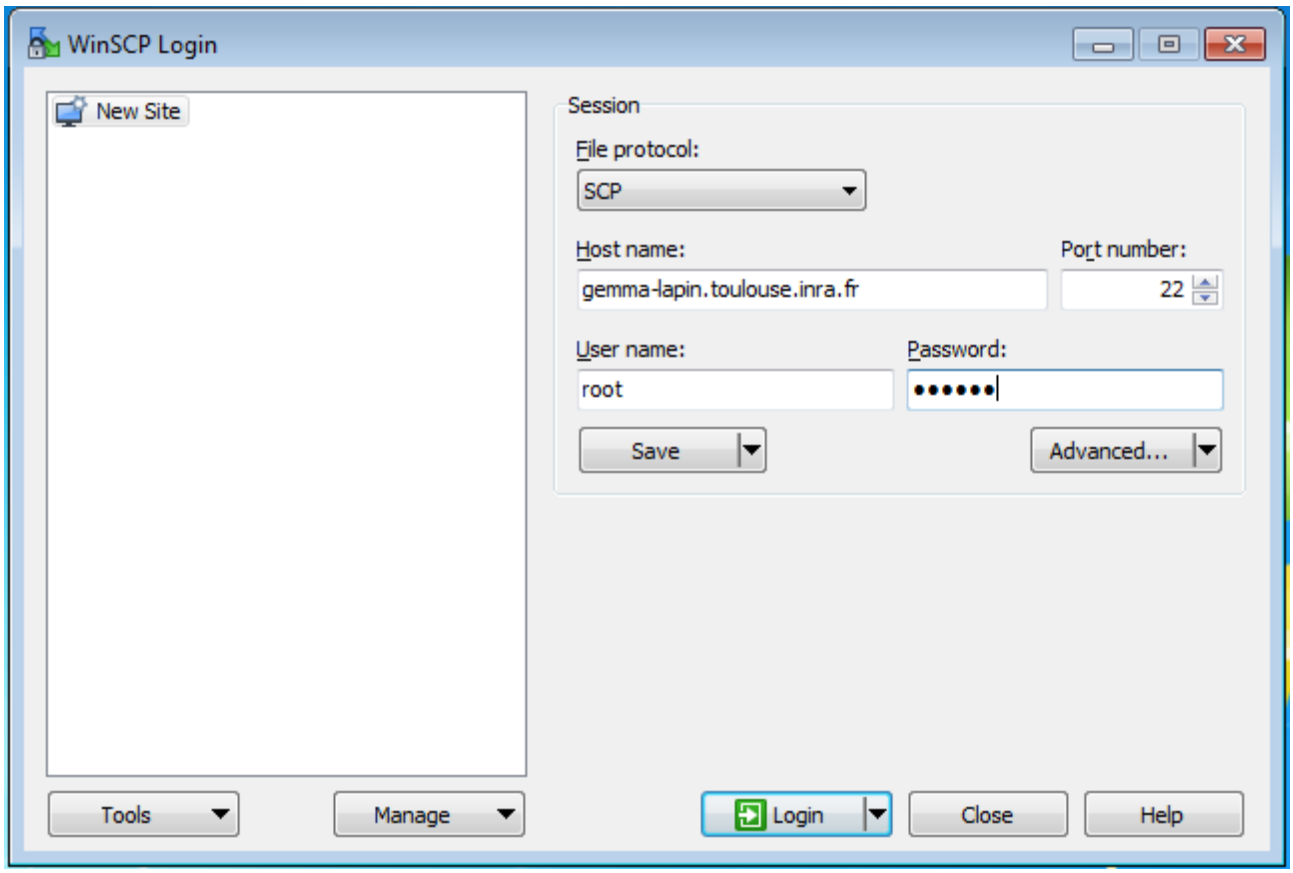


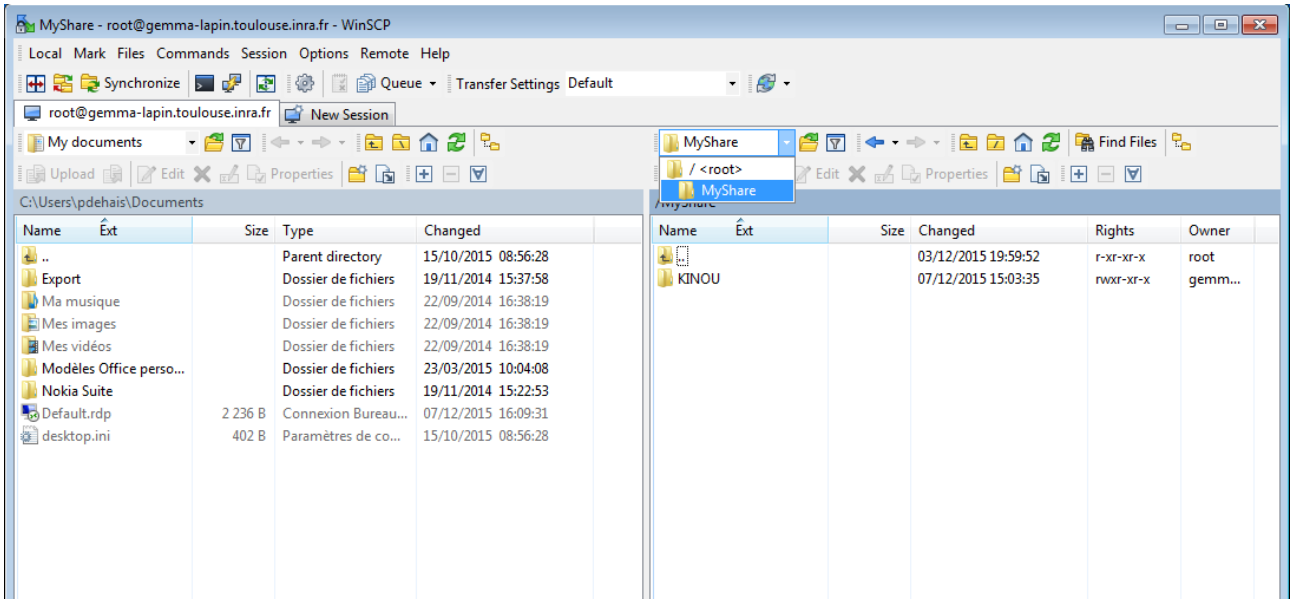
Depuis la machine Centos (ssh), le répertoire est /MyShare

```
[pdehais@inf211 ~]$ ssh root@gemma-lapin
root@gemma-lapin's password:
Last login: Mon Dec  7 09:39:18 2015 from 147.99.97.143
[root@gemma-lapin ~]# ls -lR /MyShare/
/MyShare/:
total 4
drwxr-xr-x. 4 gemmalapin gemmalapin 4096 Dec  7 15:03 KINOU

/MyShare/KINOU:
total 8
drwxr-xr-x. 2 gemmalapin gemmalapin 4096 Dec  7 15:03 New_Version
drwxr-xr-x. 2 gemmalapin gemmalapin 4096 Dec  7 15:03 Sauvegarde

/MyShare/KINOU/New_Version:
total 0

/MyShare/KINOU/Sauvegarde:
total 5068
-rwxr--r--. 1 gemmalapin gemmalapin 5182976 Dec  7 09:37 Gemma_Lapin021.4BK
-rwxr--r--. 1 gemmalapin gemmalapin     772 Dec  7 09:37 Gemma_Lapin021.4BR
[root@gemma-lapin ~]#
```

Pour les transferts de fichiers, il est donc possible de les faire via la commande scp, ou en mode graphique depuis un poste windows à l'aide de WinSCP:

(https://winscp.net/download/winscp576.zip)





La copie des fichiers se fait alors par glisser-déposer.